



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,174	05/10/2001	Johan Cornelis Talstra	NL000262	5915
24737 7590 05/07/2007 PHILIPS INTELLECTUAL PROPERTY & STANDARDS P.O. BOX 3001 BRIARCLIFF MANOR, NY 10510			EXAMINER POLTORAK, PIOTR	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 05/07/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

MAY 07 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/853,174
Filing Date: May 10, 2001
Appellant(s): TALSTRA ET AL.

James D. Leimbach
For Appellant

EXAMINER'S ANSWER

Art Unit: 2134

This is in response to the appeal brief filed 1/03/07 appealing from the Office action mailed 03/24/06.

(1) Real Party in Interest

A statement identifying by name the real party in interest as U.S. Philips Corporation is contained in the brief.

(2) Related Appeals and Interferences

The brief indicated no related appeals and interferences, which directly affect or be directly affected by or have a bearing on the decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Art Unit: 2134

- ❖ Bloom et al. (Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw, "Copy protection for DVD video", C.B.S.Proceedings of the IEEE ,Volume: 87 , Issue: 7 , July 1999 Pages:1267 - 1276),
- ❖ Glogau et al. (International Pub. No. WO 99/11020),
- ❖ Wirtz (U.S. Patent No. 5940134),
- ❖ Taguchi et al. (U.S. Patent No. 5915025),
- ❖ Robert Sedgewick, "Algorithms", second edition, 1998, ISBN: 0201066734, pg.. 35-163),

(9) Grounds of Rejection

The 35 USC § 112 rejection is withdrawn.

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of 35 U.S.C. 102(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-3, and 13-20 are rejected under 35 U.S.C. 102(a) as being anticipated by *Bloom et al. (Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw,*

Art Unit: 2134

"Copy protection for DVD video", C.B.S.Proceedings of the IEEE , Volume: 87 , Issue: 7 , July 1999 Pages:1267 - 1276).

Bloom et al.'s invention is directed to copy protection for DVD using watermarking (*Title and an Abstract*). *Bloom et al.* teach that watermarking is a technique for hiding information directly in video (*Bloom et al.*, pg. 1269 col. 1).

As per claims 1-3, 13-19 *Bloom et al.* teach an embedded watermark within DVD content that reads on a second signal logically embedded in a first signal.

Bloom et al. teach a wobble with a 64 bits payload in DVD-ROM disks (*Bloom et al.*, pg. 1275 col.1) that reads on a physical mark for storing at least part of the information on the information carrier.

Bloom et al. teach evaluation of the watermark information and the wobble information and only if the two (*information bits*) match playback is allowed (*Bloom et al.*, pg. 1275, col. 1).

This reads on refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected.

Also from the above it is clear that each single (incorrect) bit of the second signal (watermark payload) triggers an action. For example, the single incorrect bit triggers the refusal of the playback. As a result the second signal as disclosed by *Bloom et al.* includes "a single bit trigger".

Art Unit: 2134

Claims 4-7, 10-11 and 21-22 are rejected under 35 U.S.C. 103 (a) as being unpatentable over *Glogau et al.* (International Pub. No. WO 99/11020) in view of *Bloom et al.* (Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J. -P.M.G.; Miller, M.L.; Traw, "Copy protection for DVD video", C.B.S.Proceedings of the IEEE , Volume: 87 , Issue: 7 , July 1999 Pages:1267 - 1276) and *Wirtz* (U.S. Patent No. 5940134).

Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (pg. 2 lines 14-17).

Glogau et al. do not teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected.

Bloom et al. teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected as discussed above and *Wirtz* provides a motivation to combine (*Abstract and col. 2 lines 43-47*).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical

mark as taught by *Bloom et al.* in *Glogau et al.*'s invention. One of ordinary skill in the art would have been motivated to perform such a modification in order to ensure that the information preventing an illegal playback of the content is not lost when a disk is copied.

Glogau et al. in view of *Bloom et al.* do not explicitly teach the linear feedback shift register (*LFSR*) being over Galois Field. However, pseudo-random numbers generate 1s and 0s, which appear fairly random, but after certain times the numbers repeat, and for the purposes of security the interest is to extend the time of this repeat to as long as possible. The choice of a minimal and irreducible polynomial function (*such as Galois*) which gives a long time period without the repeat would have been obvious to one of ordinary skill in the art given that they are well known and barring any unexpected results.

As per claims 4-7 *Bloom et al.* teaches that the second signal is embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register.

Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted

Art Unit: 2134

packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (*pg. 2 lines 14-17*).

As per claim 21, in the XOR function 1s are ignored and 0s influence the result, which reads on "and its output is biased by interpreting emitted symbols '0'...'s-n-1' as 'unencrypted and 's-n'...'s-1' as 'encrypted'.

Glogau et al., *Bloom et al.* and *Wirtz* teach the apparatus as discussed above.

As per limitation 22 *Glogau et al.*, *Bloom et al.* and *Wirtz* do not explicitly teach embedding the second signal in the first signal by selecting a key for at least partly encrypting the information from one of at least two groups of keys.

Official Notice is taken that it is old and well-known practice to protect data signals by encrypting the data signals using encryption keys. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to embed the second signal in the first signal by selecting a key for at least partly encrypting the information from one of at least two groups of keys. One of ordinary skill in the art would have been motivated to perform such a modification in order to protect the second signal from being altered.

As per claim 10 *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not explicitly teach selecting the key from one of at least two groups of keys.

Official Notice is taken that it is old and well-known practice to have more than one key available in a system (*e.g. Taguchi et al., U.S. Patent No. 5915025*

Art Unit: 2134

teach multiple groups with multiple keys, col. 23 lines 16-29 and Fig. 25). One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ more than one key in order to provide more flexibility and compatibility for encryption using systems. In the multiple key systems selecting a key from one of at least two groups of keys is implicit.

As per claim 11 computers project all information to n-bit numbers (0s and 1s) to accommodate a particular processor used in the computers.

As per claim 12 *Glogau et al.*, *Bloom et al.* and *Wirtz* do not explicitly teach that said examining process takes the form of going down a binary tree, where said going left is caused by projection-value 0 and right by projection in value non-zero. However, Official Notice is taken that the examining process of the form of going down a binary tree, and 0/1 or 1/0 for moving left/right or right/left is old and well-known in the art of computing (e.g. *Robert Sedgewick, "Algorithms", second edition, 1998, ISBN: 0201066734, pg. 35-163*), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to do so given the benefit of implementing proven methodology.

(10) Response to Argument

Art Unit: 2134

Claim limitations and appellant arguments (and position) are presented using italic fonts.

Fonts size 10 are used to expose literal citations.

On pages 11-13, appellant addresses claims 1-3 and 13-20.

In the section "C. The differences between the invention and the references" appellant argues that there is

"no disclosure or suggestion within Bloom et al. for any action to be taken if the wobble is not detected"

and that

"Bloom et al. do not disclose or suggest any action that is taken or prevented from being taken upon the detection of the absence of a wobble groove (physical mark)".

The examiner disagrees with appellant's conclusion. It appears that appellant attempts to find a literal citation of the claim limitation in Bloom et al.'s teaching.

In particular, it appears that appellant searches for a presence of the negative limitation and overlooks the meaning of a positive recitation offered by Bloom et al.

The examiner points to pg. 1275, col. 1 lines 28-37, wherein Bloom et al. recites as follows:

"A coarse description of playback control with a wobble is as follows. Upon insertion of a disk in a compliant drive, the drive will look for the presence of a wobble, and if present read out the 64

Art Unit: 2134

bits of payload. If the (compliant) MPEG decoder informs the drive that a copy-never watermark is read, the drive: 1) feeds the 64 wobble bits through the one-way function F and 2) requests the MPEG decoder to read out the additional payload of the watermark. Only if the additional watermark payload and transformed wobble bits match is playback allowed."

The wobble reads on a physical mark and an ordinary artisan would readily recognize that the positive statement "only if ... is playback allowed" is equivalent to appellant's argued "*action that is taken or prevented from being taken upon the detection of the absence of a wobble groove (physical mark)*".

Appellant concludes the section "C. The differences between the invention and the references" stating:

"The rejection contradicts itself. The appellants, respectfully, point out that is impossible for Bloom et al. to anticipate the rejected claims because the subject matter for the second signal but no physical mark is detected is not disclosed or suggested by Bloom et al."

The examiner disagrees with appellant conclusion. Once again, it appears that appellant attempts to search for a literal citation of argued limitation in Bloom et al.'s reference. Furthermore, it appears that while analyzing limitations appellant disregards the overall contextual meaning.

The examiner would like to emphasize the entire meaning of the whole limitation:

"refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected".

As indicated in the previous Office Action examiner considers a watermark (watermark information/payload) disclosed by Bloom et al. to correspond to a second signal. On pg. 1275, col. 1 lines 28-37, Bloom et al. disclose:

"A coarse description of playback control with a wobble is as follows. Upon insertion of a disk in a compliant drive, the drive will look for the presence of a wobble, and if present read out the 64 bits of payload. If the (compliant) MPEG decoder informs the drive that a copy-never watermark is read, the drive: 1) feeds the 64 wobble bits through the one-way function F and 2) requests the MPEG decoder to read out the additional payload of the watermark. Only if the additional watermark payload and transformed wobble bits match is playback allowed."

There is not contradiction and no mistakes: the reference clearly suggests that the playback occurs when the second signal and physical mark are present and clearly suggests that the playback is not allowed when a second signal is detected but physical mark is not, because no matching between the additional watermark payload and transformed wobble bits occurs.

On pages 13-18, appellant contests the rejection of claims 1-3 and 13-20 over Bloom et al.

Although appellant starts each claim with recitation of the claim limitations, appellant does not offer any arguments to validate appellant assumption that *"there is not disclosure*

Art Unit: 2134

or suggestion within Bloom et al. for ...". Appellant's factual counter arguments seem to be replaced with the second copy of the claim language.

For example, note the entire paragraph cited against claim 2:

"Appealed claim 3 defines the subject matter for an apparatus according to appealed claim 1, wherein the physical mark is a wobble. There is no disclosure or suggestion within Bloom et al. for an apparatus according to appealed claim 1, wherein the physical mark is a wobble".

This leads examiner to believe that appellant overlooked some of Bloom et al.'s disclosure, and as a result failed to identify the cited fragments as relevant to appellant's limitations.

Since appellant arguments consists of only repeating the claim language, the examiner assumes that appellant requests a plain guide to Bloom et al.'s teaching.

For purpose of clarity the examiner explains reference to claims 1-3 and 13-20 in order from the broadest to the narrowest.

The examiner presents claim in following order: 13, 2, 16, 20, 19, 17-18, 3, 15 and 1.

Claim 13 limitations:

"detecting a second signal logically embedded in the first signal

wherein the second signal contains an encrypted trigger,

detecting a physical mark

used for storing at least part of the information on the information carrier, and

Art Unit: 2134

refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected".

Bloom et al.'s invention is directed to copy protection for DVD using watermarking (Title and an Abstract). Bloom et al. teach that watermarking is a technique for hiding information directly in video (Bloom et al., pg. 1269 col. 1). The embedded watermark (watermark information/payload) embedded within protected content corresponds to a second signal logically embedded in a first signal.

The previously discussed Bloom et al.'s col. 1 lines 28-37 (pg. 1275), discloses that the physical mark (wobble) stores at least part of the information stored on an information carrier and that the physical mark and a second signals are detected ("the drive will look for the presence of a wobble", "read out the 64 bits of payload" etc.), and *"refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected"*.

The examiner also points out that even if Bloom et al. did not disclose detection of the physical mark and the signal, an ordinary skilled artisan would readily recognize that interpreting (e.g. reading) information by computer systems would not be possible without detecting the information.

Claim 2 limitations:

"wherein the physical mark is a wobble"

See pg. 1275, col. 1 line 30, for example.

Claim 16 limitations:

"using a physical mark for storing at least part of the information on the information carrier, and logically embedding a second signal in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier, the second signal containing a single bit trigger that may be used for refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected."

In addition to limitations discussed in regard to claim 13 the examiner points out that an ordinary artisan would understand that in order for the second signal to be embedded in the first signal, the step of embedding must have occurred.

Furthermore, the examiner points to col. 1 lines 28-37 (pg. 1275) in light of the last paragraph on pg. 1274, specifically:

"A ticket T is a cryptographic counter, which is implemented as a multibit random number. The counter value $\langle T \rangle$ depends on the presence of a watermark W with a multibit payload $\langle W \rangle$ and is defined as the number n such that $F^n(T) = \langle W \rangle$. Here, $F(\cdot)$ denotes a fixed and secure cryptographic one-way function."

The disclosure clearly suggests that the second signal contains at least one single bit. Thus, any incorrect one single bit of the second signal (watermark payload) would result in (trigger) playback refusal (recall that "only if the additional watermark payload and transformed wobble bits match is playback allowed.").

Art Unit: 2134

Additionally the examiner points out that even if Bloom et al. did not disclose that the second signal comprised a single bit, an ordinary skilled artisan would readily recognize that any information (in order to exist/being interpreted by a computer) must include at least one bit, which is the smallest unit holding computing values.

Furthermore, the examiner points out that even if Bloom et al. did not disclose that the single bit was used for refusing play back of the information read from the information carrier, the term "can" used by appellant in the claim limitation constitutes of a non positive recitation requiring that the method has only the capability to perform a particular functions not that it actually performs them. Similarly, the term "for" could be considered as an intended use limitation.

Claim 20 limitations:

"an apparatus for storing information on an information carrier as claimed in claim 14 and an apparatus for reading out information from an information carrier, wherein the copy protection information including a second signal logically embedded in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier is exchanged between both apparatuses, which copy protection information may be used for refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected."

Bloom et al. disclosure

"upon insertion of a disk in a compliant drive, the drive will look for the presence of a wobble ..." unmistakably indicates an apparatus for storing information on an information carrier and an apparatus for reading out information form an information carrier. Appellant is

Art Unit: 2134

also encouraged to examine Fig. 5 on pg. 1275 (or Fig. 2 on pg. 1269) as well as the remaining teaching of Bloom et al. wherein a player and a recorder are repeatedly addressed.

Lastly, as per copy protection issue, the examiner points out that even the title of Bloom et al.'s reference indicates that the teaching is directed towards a copy protection concept.

Claim 19 limitations

are substantially similar to previously discussed claims.

Claim 17 limitations

are directed towards an information carrier comprising:

"a physical mark for storing at least part of the information on the information carrier, and a second signal logically embedded in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier, the second signal containing a single bit trigger that may be used for refusing play back of the information read from the information carrier if a second signal but no physical mark has been detected"

and

Claims 18 limitations

recite:

"wherein the information carrier is a CD-or a DVD-disc."

Art Unit: 2134

Bloom et al. explicitly recites that the carrier is a DVD-ROM (pg. 1275, col. 1 lines 16).

Furthermore, the examiner points out that even though the intended use recitations (e.g. "a physical mark for storing at least part of the information on the information carrier") recited by claim 17 are disclosed by Bloom et al. (including "at least partly encrypted content" – the content the value of which could only be retrieved the one-way function or cryptographically secured CGMS, see the last paragraph of pg. 1274), the recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)).

Claims 2 and 15 limitations:

"wherein the apparatus is a CD-or a DVD-player"

In addition to previously discussed Bloom et al.'s disclosure naming DVD-ROM as a carrier read by a player/recorder, in the "Introduction" section (pg. 1267) Bloom et al. clearly disclose DVD players implementing the copy protection.

Claims 1 limitations

are substantially similar to previously discussed limitations.

The only point to be made, regarding claim 1, is that the structure of the apparatus as indicated by appellant disclosed "means" is a typical structure of a digital disk player

Art Unit: 2134

(such as DVD player). For example, digital disks comprise tracks read by a reading heads that use optical systems implementing a focus lights (lasers). In order to read disk tracks the digital disks are rotated. The disk data is read by detecting different phases (values) and the light implemented is reflected by the disks, etc.

Summary of discussion above:

Bloom et al.'s reference clearly reads on the limitations of claims 1-3 and 13-20.

On pages 18-22, appellant addresses claims 4-7, 10-11 and 21-22.

On pg. 20-21 of the "C. The differences between the invention and the references" section appellant does not explicitly provide the claim that appellant's argument pertains to.

However, it appears that appellant once again returns to the previously argued limitation, addressing a physical mark used for storing information on the information carrier and refusing playback of the second signal but no physical mark has been detected. For example, the appellant argues:

"the construction made by the rejection is an impossible construction. The appealed claims define subject matter for 'if a second signal but no physical mark is detected'. The appealed claims can not be read so broadly to as to encompass the wobble groove as the first signal because this would not be possible to in view of the working of the rejected claims"

and

"there is no disclosure or suggestion within Bloom et al. for a second signal that is logically embedded in the first signal indicating that a physical mark is used for storing at least part of the information on the information carrier... the second signal to contain a single bit trigger that may be used for refusing play back of the information read from the information carrier if a second signal but no physical mark has been detected".

The second signal logically embedded in the first signal indicating physical mark used for storing at least part of the information on the information carrier, containing a single bit trigger that could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark is detected is addressed above (in regard to claims 1-3 and 13-20).

However, the examiner would like to once again caution appellant to review cited limitations in the full context rather than analyze fragments in a vacuum.

As discussed above, Bloom et al.'s invention is directed to copy protection for DVD using watermarking (Title and an Abstract). Bloom et al. teach that watermarking is a technique for hiding information directly in video (Bloom et al., pg. 1269 col. 1). A second signal logically embedded in a first signal (the embedded watermark information/payload within protected content) as well as Bloom et al.'s disclosure (pg. 1274-1275):

"A coarse description of playback control with a wobble is as follows. Upon insertion of a disk in a compliant drive, the drive will look for the presence of a wobble, and if present read out the 64 bits of payload. If the (compliant) MPEG decoder informs the drive that a copy-never watermark

Art Unit: 2134

is read, the drive: 10 feeds the 64 wobble bits through the one-way function F and 2) requests the MPEG decoder to read out the additional payload of the watermark. Only if the additional watermark payload and transformed wobble bits match is playback allowed."

and

"A ticket T is a cryptographic counter, which is implemented as a multibit random number. The counter value $\langle T \rangle$ depends on the presence of a watermark W with a multibit payload $\langle W \rangle$ and is defined as the number n such that $F^n(T) = \langle W \rangle$. Here, $F(\cdot)$ denotes a fixed and secure cryptographic one-way function."

suggests no contradiction, but instead unambiguously indicate a second signal logically embedded in a first signal indicating physical mark used for storing at least part of the information on the information carrier, containing a single bit trigger that could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark is detected.

(For complete discussion refer to examiner's remarks regarding claims 1-3 and 13-20, above.)

On pg. 21 of appellant extensively argues Wirtz's disclosure, stating for example:

"The rejection alleges that Wirtz in the Abstract and col. 2, lines 43-47 teaches that the first signal/physical mark in which a second signal is logically embedded and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected"

Art Unit: 2134

It appears that appellant extracted fragments of the rejection out of context. Wirtz reference was offered only to provide motivation to combine rather than, as appellant alleges, to disclose *"the first signal/physical mark in which a second signal is logically embedded and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected"*.

For appellant convenience, the examiner provides Wirtz's relevant teaching (In col. 2 lines 43-47 (Abstract)):

"The watermark is not lost when the signal is re-encoded and copied on a recordable disc. A player will not reproduce the copy because the watermark no longer corresponds with the 'wobble key' of the new disc".

and previously cited rejection:

"Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (pg. 2 lines 14-17).

Glogau et al. do not teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected.

Bloom et al. teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected as discussed above and

Wirtz provides a motivation to combine (Abstract and col. 2 lines 43-47).

It would have been obvious to one of ordinary skill in the art at the time of appellant's invention to incorporate a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second

signal but no physical mark as taught by Bloom et al. in Glogau et al.'s invention. One of ordinary skill in the art would have been motivated to perform such a modification in order to ensure that the information preventing an illegal playback of the content is not lost when a disk is copied."

Teaching of Bloom et al.'s physical mark has been already discussed above.

On pg. 22 appellant asserts that the observation that the choice of a minimal and irreducible polynomial function would have been obvious to a person of ordinary skill within the art would amount to no more than a statement not sufficient to establish a prima facie case of obviousness. Furthermore, appellant appears to contest interpretation of Glogau et al.'s as disclosing one signal being embedded in another (second signal embedded in first signal) by encoding in a pseudo-random noise pattern in encrypted and unencrypted packets of the first signal, wherein the encryption sequence is generated based on a linear feedback register.

However, appellant admits finding in Glogau et al.'s disclosure that the encryption sequence is substantially random, that can be generated based on a linear feedback register and that the encryption sequence is embedded into the carrier signal by performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

Appellant arguments are not understood. The examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation

Art Unit: 2134

to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, an ordinary artisan would readily recognize that Galois field (GF) not only represents irreducible polynomial function but also that GF is well known (if not fundamental) and widely implemented in the art of computing (in particular in the art of computer security/watermarks).

Furthermore, as indicated in the previous Office Action regarding the pseudo-random numbers (taught by Glogau et al.), a skilled ordinary artisan would recognize that pseudo-random functions generate 1s and 0s, which appear fairly random, but after certain times the numbers repeat posing a potential security threat. Thus, for the purposes of security the interest is to extend the time of this repeat to as long as possible. A skilled artisan would also recognize that an irreducible polynomial function (*such as Galois*) yields a long time period without the repeat. As a result the choice of implementing an irreducible polynomial function would have been obvious to one of ordinary skill in the art given that benefit of increased security as well as being well known and barring any unexpected results.

Furthermore, a skilled artisan would readily recognize that using a signal (such as a pseudo-random noise pattern) to encode another signal is equivalent to embedding one signal within another one.

On pg. 23-27 appellant addresses claims 4-7, 10-12 and 21-22.

In regard to claims 4-5, appellant offers two copies of claim limitations and argues previous point of refusing play back of the information read from the information carrier if the second signal but no physical mark has been detected.

As cited in the previous Office Action Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (pg. 2 lines 14-17).

The examiner points out that pseudo-random is not the same as random. An ordinary artisan would recognize that pseudo-random patterns used for encoding are superficially generated to appear to be random (e.g. by a pseudo-random number generators, which use a seed and a pseudo-random number algorithm). Thus the pseudo-random pattern reads is a predetermined pattern.

Although Glogau et al. do not teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark has been detected, Bloom et al. teach a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information

Art Unit: 2134

carrier if the second signal but no physical mark has been detected as discussed above and Wirtz provides a motivation to combine (Abstract and col. 2 lines 43-47).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate a physical mark used for storing at least part of the information on the information carrier and refusing playback of the information read from the information carrier if the second signal but no physical mark as taught by Bloom et al. in Glogau et al.'s invention. One of ordinary skill in the art would have been motivated to perform such a modification in order to ensure that the information preventing an illegal playback of the content is not lost when a disk is copied.

In regard to claims 6-7 appellant offers only two copies of claim limitations.

The examiner refers applicant to the original rejection which points to Glogau et al.'s teaching of the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (Glogau et al., pg. 2 lines 14-17).

Although Glogau et al. in view of Bloom et al. do not explicitly teach the linear feedback shift register (*LFSR*) being over Galois Field the examiner pointed out that pseudo-random numbers generate 1s and 0s, which appear fairly random, but after certain times the numbers repeat, and for the purposes of security the interest is to extend the time of this repeat to as long as possible. The choice of a minimal and irreducible

Art Unit: 2134

polynomial function (*such as Galois'*) which gives a long time period without the repeat would have been obvious to one of ordinary skill in the art given that they are well known and barring any unexpected results.

As per claim 10 appellant argues that although Taguchi et al. (U.S. Patent No. 5,915,025) illustrates the well known concept of multiple groups with multiple keys, "Taguchi et al. do not disclose an apparatus as defined by claim 10, wherein a key detection algorithm is used to select the key and to decode from which group of keys said key has been selected an apparatus as defined by claim 11, wherein the decoding algorithm comprises an examining process of the outcome of projecting an n-bit key onto a set of fixed n-bit numbers."

It appears that applicant argues limitations not present in claims 10. The examiner clarifies that claim 10 recites:

"wherein a key detection algorithm is used to select the key and to decode from which group of keys said key has been selected".

As indicated in the previous rejection although Glogau et al. in view of Bloom et al. and Wirtz do not explicitly teach selecting the key from one of at least two groups of keys the examiner took Official Notice that it is old and well-known practice to have more than one key available in a system (e.g. Taguchi et al., U.S. Patent No. 5915025 teach multiple groups with multiple keys, col. 23 lines 16-29 and Fig. 25) and that one of ordinary skill in the art at the time of applicant's invention would have been motivated to

Art Unit: 2134

employ more than one key in order to provide more flexibility and compatibility for encryption using systems. In the multiple key systems selecting a key from one of at least two groups of keys is implicit (the appropriate/corresponding key must be used in the decryption process to obtain the original data).

As per claim 11 appellant appears to repeat the claim language as allegedly not found in Glogau et al. in view of Bloom et al. and further in view of Wirtz's rejection.

In order to address limitations of claim 11 reciting "wherein the decoding algorithm comprises an examining process of the outcome of projecting an n-bit key onto a set of fixed n-bit numbers" the examiner pointed out that computers project all information to n-bit numbers (0s and 1s) in order to accommodate a particular processor used in the computers. Also, the decoding algorithm uses only particular values (a key and a values to be decrypted). This discriminate process of selecting data by itself reads on the broad term such as "an examining process".

As per claim 12 appellant argues that although Sedgwick illustrated a well known concept of binary trees for efficient searching, "Sedgewick does not disclose or suggest an examining process that takes the form of going down a binary tree, where said going left is caused by projection-value 0 and right by projection in value non-zero".

Art Unit: 2134

The examiner is not sure what exactly needs to be clarified. Binary trees are a fundamental structure implemented by computing algorithms, including algorithms implementing searching. During a search process a binary tree is "traveled" using a path consisting of values that match a particular criteria. Traveling a binary tree starts from the root of the tree and inherently has a choice of moving down to the right or left. A computer acts only upon instructions (even an outside events are interpreted and act upon using computer instructions). Thus an instruction to move right or left must be provided to the computer. Since in a computer everything is accomplished using a numerical value, 0 could be used to represent left and 1 to represent right (or vice a versa), either representation being a obvious variation of each other and selecting any one of them for right or left would not affect the functionality of the invention.

As per claim 21 appellant appears appellant argues that Glogau et al. in view of Bloom et al. and further in view of Wirtz does not disclose the linear feedback shift register over GF, and its output 1/s biased by interpreting emitted symbols "0"...'s-n-1' as 'unencrypted' and 's-n' ...'s-1' as encrypted.

Furthermore, Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (pg. 2 lines 14-17).

Art Unit: 2134

Since the decryption process is a reverse of encryption process the encrypted and unencrypted packs will be subject to evaluation of which of the packs to be decrypted.

The process will be biased decrypting only encrypted packs. Also, a pack of values will have a starting position (e.g. "0" for the first pack, in computers the process of counting frequently begins at "0", see one of the most popular C++ or Java, computer languages, for example) and an ending position (e.g. "s-n-1"). The next pack will start at the following value (in this case 's-n').

Lastly, in the processing data that comprises mixed packs has inherently only two choices: starting with unencrypted pack followed by the encrypted pack or vice versa. Each one of the choices would have been an obvious variation not affecting the functionality of the invention.

Selecting an unencrypted pack as a first pack would read on claim 21 limitations.

As per claim 22 appears to draw attention to the fact that no support was provided to illustrate the concept of selecting a key for at least partly encrypting the information from one of at least two groups of keys.

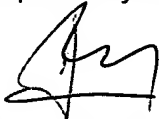
As previously discussed although Glogau et al. teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (pg. 2 lines 14-17), Glogau et al.

Art Unit: 2134

in view of Bloom et al. and Wirtz do not explicitly teach selecting the key from one of at least two groups of keys. However, the examiner took Official Notice that it is old and well-known practice to have more than one key available in a system (e.g. Taguchi et al., U.S. Patent No. 5915025 teach multiple groups with multiple keys, col. 23 lines 16-29 and Fig. 25) and that one of ordinary skill in the art at the time of applicant's invention would have been motivated to employ more than one key in order to provide more flexibility and compatibility for encryption using systems. In the multiple key systems selecting a key from one of at least two groups of keys is implicit (the appropriate/corresponding key must be used in the encryption/decryption process to obtain the original data). It is also implicit that once selected, the key is used to encrypt/decrypt data.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,



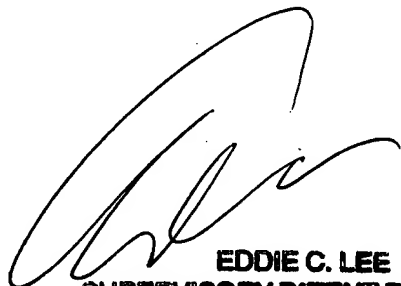
Peter Poltorak

Conferees:


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

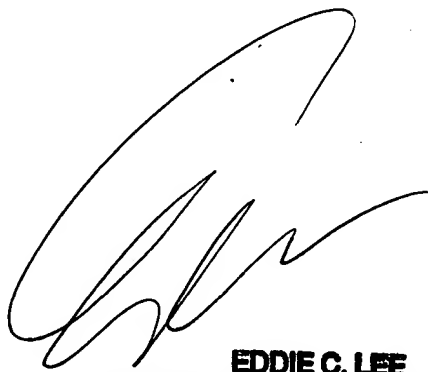
Kambiz Zand

Eddie Lee.


EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

A handwritten signature in black ink, appearing to be 'E. Lee', with a large, sweeping initial 'E'.

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER